# Breach Notification SOP Overview and Activity

## Your Role as the "Human Firewall"

**2008 Data Protection Seminar**

**TMA Privacy Office**

# Purpose

- Define the process for individuals responsible for assessing and handling a breach that affects TRICARE Management Activity (TMA), as elaborated in the sections within the Standard Operating Procedure (SOP) for Breach Notification

# Objectives

- This presentation will:
  - Explain the key elements of breach response and notification
  - Define your role in identifying and responding to breaches
  - Describe how to prevent breaches and protect your identity

# Agenda

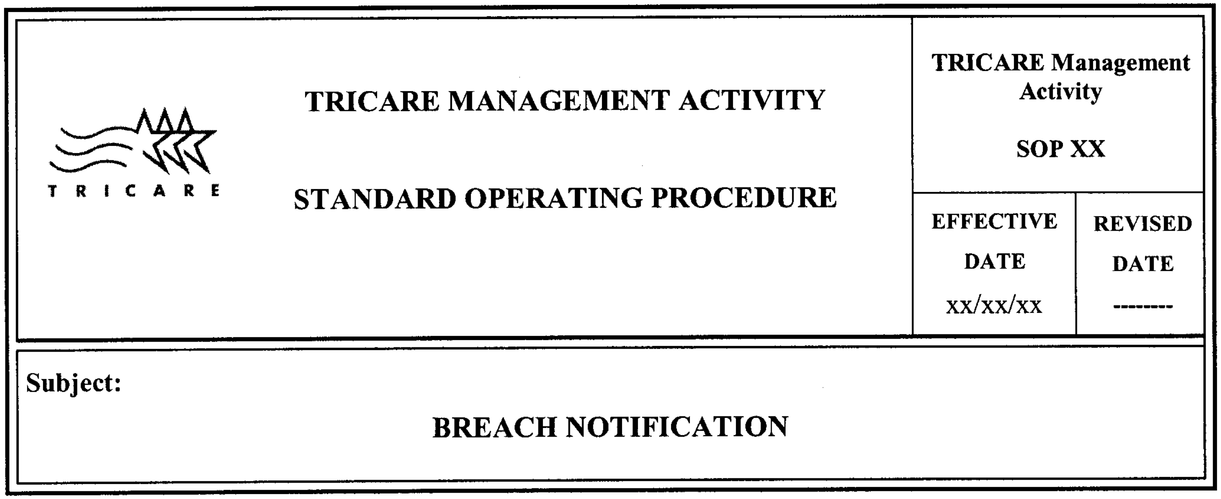
- Background
- The Main Sections of the SOP
    - Roles and Responsibilities
    - Procedures
    - Enclosures
- Activity
- Best Practices

# Background

Breach Notification SOP Overview and Activity

# Implementation

- The TMA Incident Response SOP for Breach Notification was signed on October 12, 2007
  - Along with the "TRICARE Management Activity Incident Response Team and Breach Notification Policy Memorandum"



| | | | |
|---|---|---|---|
| TRICARE | TRICARE MANAGEMENT ACTIVITY<br>STANDARD OPERATING PROCEDURE | TRICARE Management Activity<br>SOP XX | |
| | | EFFECTIVE DATE<br>xx/xx/xx | REVISED DATE<br>-------- |

Subject:

BREACH NOTIFICATION

Breach Notification SOP Overview and Activity

# Scope of the SOP

- Applies to all TMA workforce members, including:
  - TMA Directorates
  - TRICARE Regional Offices (TROs)
  - TRICARE Area Offices (TAOs)
  - All other organizational entities in TMA

Breach Notification SOP Overview and Activity

# Sensitive Information

- **Sensitive Information** is the information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under **5 U.S.C. Section 552a** (the Privacy Act of 1974), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy

Breach Notification SOP Overview and Activity

# Sensitive Information

- Sensitive Information sub-categories may include:
  - For Official Use Only (FOUO)
  - Privacy Data
  - Proprietary Information
  - Budget Information
  - Financial Data
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Electronic Protected Health Information (ePHI)

# Personally Identifiable Information (PII)

- **Personally Identifiable Information (PII)** is information about an individual that identifies, links, relates, is unique to, or describes him or her, (e.g., a Social Security Number (SSN); age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic information; biometrics; personnel, medical, and financial information)

Source: DoD 5400.11-R, "DoD Privacy Program," May 14, 2007

Breach Notification SOP Overview and Activity

# Examples of PII

- Name
- Age
- SSN
- Biometric Records
- Marital Status
- Race

- Date and Place of Birth
- Home and/or Work Phone Numbers
- Military Rank or Civilian Grade
- Salary
- Other Personal information linked to a specific individual

# Protected Health Information (PHI)

- **Protected Health Information (PHI)** – Health information that:
    - Was created or received by a covered entity, such as health care provider or health plan
    - Relates to the past, present, or future physical or mental health of an individual
    - Relates to providing health care to an individual
    - Relates to the past, present, or future payment for providing health care to an individual
    - Can be used to identify the individual

Source: DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003

# Electronic Protected Health Information (ePHI)

- Electronic Protected Health Information (ePHI) – Any PHI which is created, stored, transmitted, or received electronically on any medium, including:
  - Personal computers with their internal hard drives used at work, home, or traveling
  - External portable hard drives, including iPods
  - Magnetic tape or disks
  - Removable storage devices such as USB memory sticks/keys, CDs, DVDs, and floppy diskettes
  - PDAs, Smartphones
  - Electronic transmission includes data exchange (e.g., email or file transfer) via wireless, ethernet, modem, DSL, or cable network connections

Breach Notification SOP Overview and Activity

# What is a Breach?

Lost, stolen or compromised information, otherwise termed a **breach** is the actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected

Source: DoD 5400.11-R, “DoD Privacy Program,” May 14, 2007

Breach Notification SOP Overview and Activity

# Examples of Breaches

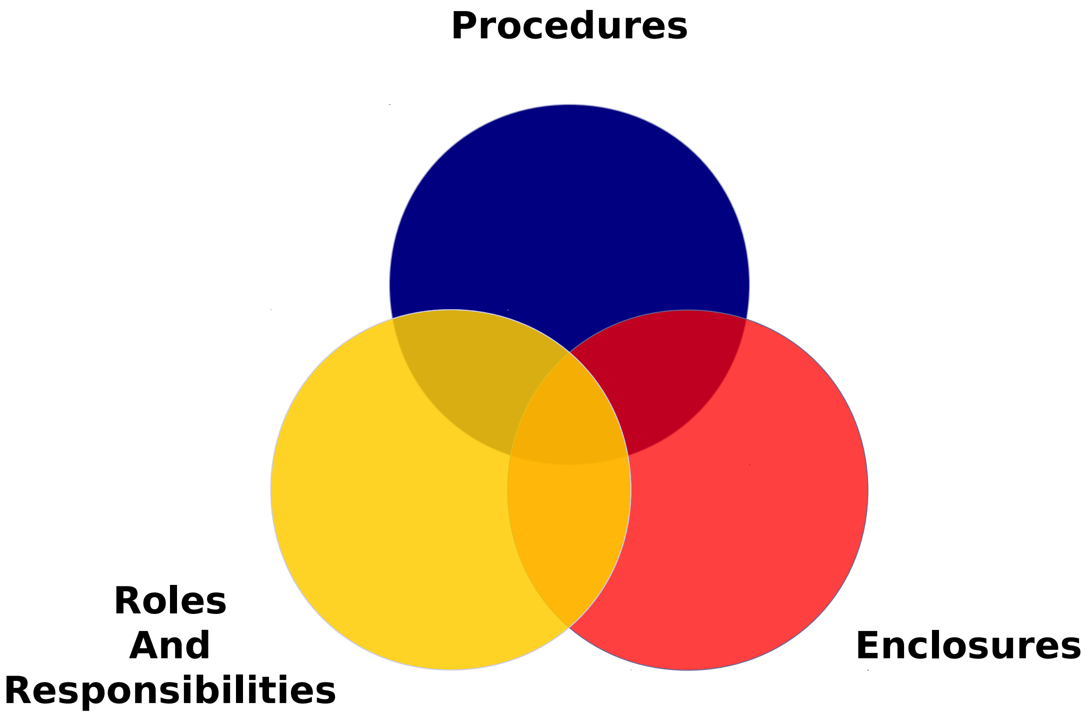
Breaches of PII and PHI may include:

- Misdirected fax documents
- Unsecured mailing or transporting of documents
- Lost or stolen removable media devices
- Transmission of unsecured emails and unencrypted files

# The Main Sections of the SOP

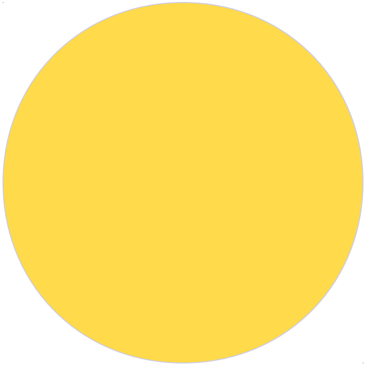
Breach Notification SOP Overview and Activity

# The Main Sections of the SOP



Breach Notification SOP Overview and Activity

# The Main Sections of the SOP



**Roles And Responsibilities**

Breach Notification SOP Overview and Activity

# Roles and Responsibilities

- This section outlines the expectations for each Program Office when handling a breach
- Roles may be fulfilled by:
  - Government employees
  - Military members
  - Contractor employees

# Pertinent Roles and Responsibilities of the Incident Response Team (IRT) Chair

- Serve as the POC for the IRT
- Ensure compliance with reporting requirements
- Ensure all IRT members have the SOP
- Report details of the breach to the IRT
- Delegate mitigation tasks
- Determine severity level based on analysis of breach

Breach Notification SOP Overview and Activity

# Pertinent Roles and Responsibilities of the IRT Chair

**(continued)**

- Update Senior Leadership and the IRT as new information becomes available
- Assign responsibilities for the development of the After Action Report
- Debrief Senior Leadership
- Assign Action Officers

Breach Notification SOP Overview and Activity

# Roles and Responsibilities of Action Officers

- Create and provide the following to the Chairman:
  - Summary of breach
  - Meeting Minutes
  - Updates for Senior Leadership
  - Executive Summaries
  - Reports to external agencies, as necessary
  - Plan of Action and Milestones
  - Notebook of chronology of actions taken

Further duties of the Action Officers can be found on page 8 of the SOP

# Roles and Responsibilities of the TMA Privacy Officer

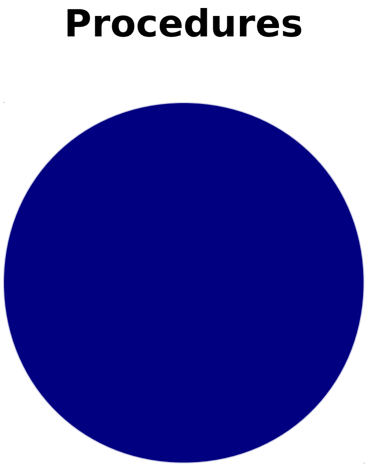
- Notify and coordinate with the IRT Chair
- Provide guidance and oversight to the IRT Chair throughout the breach notification process to ensure compliance with:
  - Incident reports
  - Updates to leadership
  - Internal/external communications
- Ensure compliance with internal incident response plan
- Conduct training for IRT representatives at least annually

# What Are Your Responsibilities?

- As an employee, you need to be able to:
  - Identify the incident
  - Obtain relevant information about the incident or potential breach
  - Notify your supervisor
- You might have additional responsibilities as elaborated in the Incident Response SOP, depending on your job function or position

Breach Notification SOP Overview and Activity

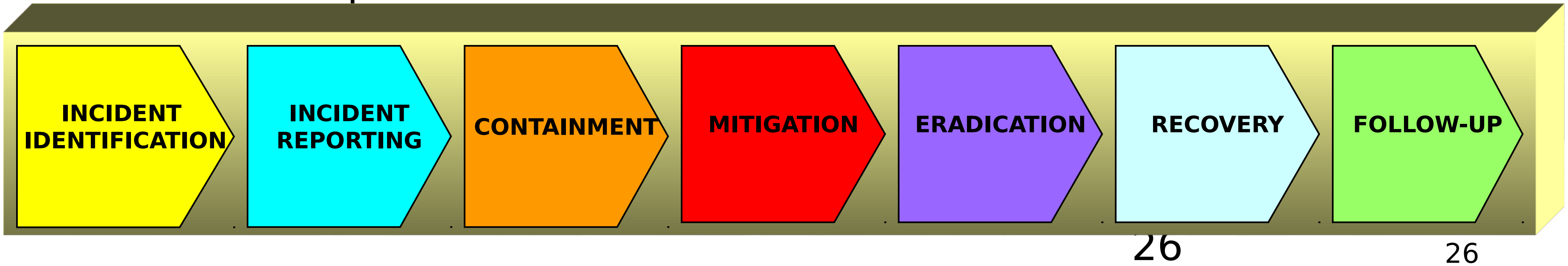
# The Main Sections of the SOP



Breach Notification SOP Overview and Activity

# Incident Response Plan Steps

- An effective Incident Response Plan includes the following steps:
  - Incident Identification
  - Incident Reporting
  - Containment
  - Mitigation
  - Eradication
  - Recovery
  - Follow-up

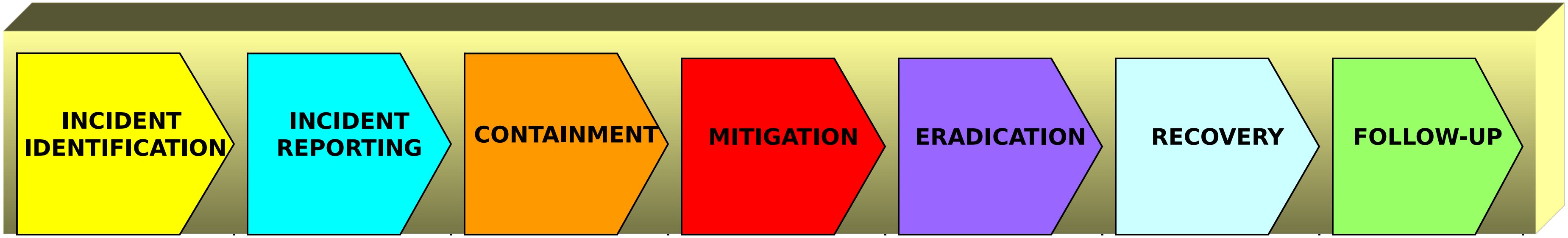


Breach Notification SOP Overview and Activity

# Incident Identification

INCIDENT IDENTIFICATION

- Incident identification involves the analysis of all available information in order to determine if an incident has occurred
- Analyze situations that may indicate that an incident has occurred
    - □ Is it a suspected or confirmed incident?
    - □ What is the evidence?
    - □ Where did it happen?
    - □ What is the extent?
    - □ What other information is needed?



INCIDENT REPORTING

Breach Notification SOP Overview and Activity

# Incident Reporting

When a breach occurs it shall be reported to the appropriate levels of leadership, both internal and external to the component

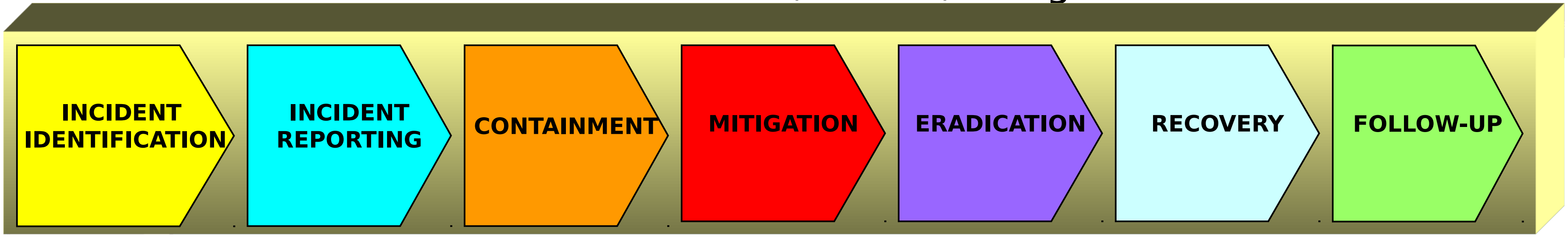
<table>
<tr><th>TMA Components</th><th>Non-TMA Components</th></tr>
<tr><td>● Leadership – Immediately<br>● TMA Privacy Office – Within 1 Hour<br>● US CERT – Within 1 Hour<br>● Component Head – Within 24 Hours<br>● DoD Privacy Office – Within 48 Hours</td><td>● Leadership – Immediately<br>● US CERT – Within 1 Hour<br>● Sr. Component Officials for Privacy – Within 24 Hours<br>● TMA Privacy Office – Within 24 Hours<br>● DoD Privacy Office – Within 48 Hours</td></tr>
<tr><td colspan="2"><b>Note: Notify issuing banks if government issued credit cards are involved; law enforcement, if necessary; and all affected individuals within 10 working days of breach and identity discovery, if necessary.</b></td></tr>
</table>

INCIDENT REPORTING

Breach Notification SOP Overview and Activity

# Incident Reporting

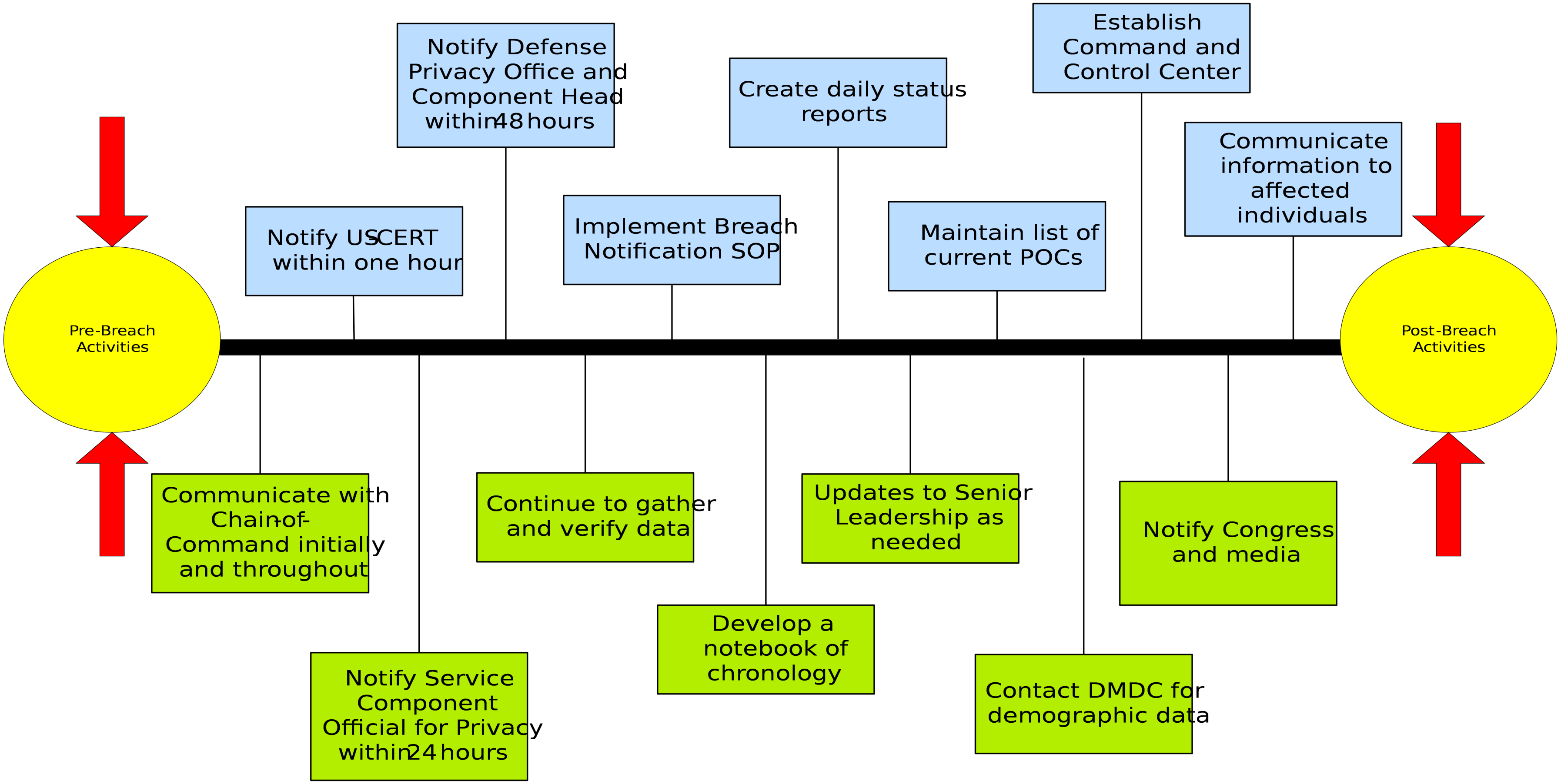
- **Communicate** with affected individuals, investigators, DoD leadership, Congress, the media (both paper and television), law enforcement agencies, and other governmental parties as necessary
- Stakeholders include:
  - **Internal:** DoD Leadership, Service Medical Departments, General Counsel
  - **External:** affected individuals, Media, Congress



## Breach Notification SOP Overview and Activity

# 10 Day Response Timeline

10 Day Breach Response Activities Timeline



Pre-Breach Activities

Communicate with Chain-of-Command initially and throughout

Notify US-CERT within one hour

Notify Service Component Official for Privacy within 24 hours

Notify Defense Privacy Office and Component Head within 48 hours

Continue to gather and verify data

Implement Breach Notification SOP

Develop a notebook of chronology

Create daily status reports

Updates to Senior Leadership as needed

Maintain list of current POCs

Contact DMDC for demographic data

Establish Command and Control Center

Notify Congress and media

Communicate information to affected individuals

Post-Breach Activities

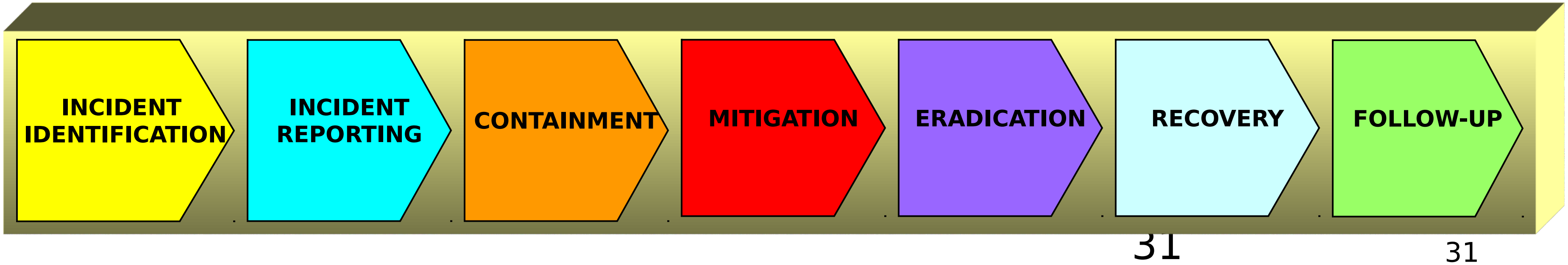
* Activities are not all inclusive nor in a specific order

Breach Notification SOP Overview and Activity

# Containment

CONTAINMENT

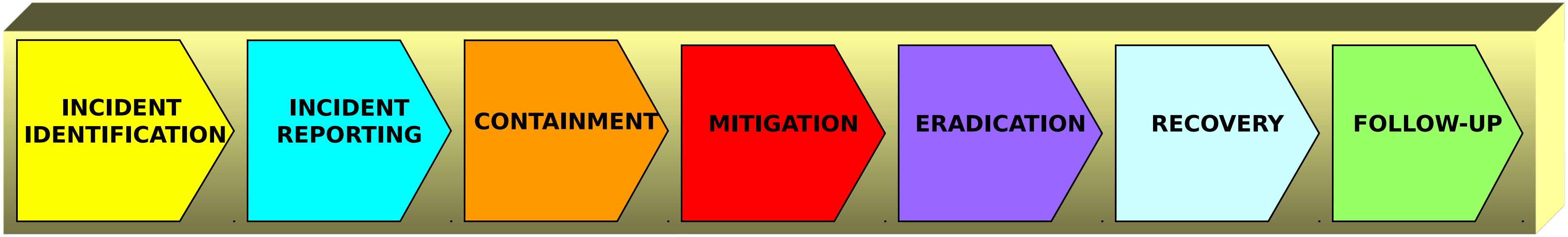
- Containment involves short-term actions that are immediately implemented in order to limit the scope and magnitude of an incident
- Containment activities include, at a minimum, the following:
  - **Identify** a course of action concerning the operational status of the compromised system or critical information
  - **Validate** whether the PHI should be left on information systems or if possible, whether it should be copied to alternative media and the system taken off-line


INCIDENT IDENTIFICATION
INCIDENT REPORTING
CONTAINMENT
MITIGATION
ERADICATION
RECOVERY
FOLLOW-UP

MITIGATION

# Breach Notification SOP Overview and Activity
# **Mitigation**

- Mitigation of harmful effect of all incidents to include both electronic and paper documents:
  - □ Securing the information/taking the affected system off-line as soon as possible
  - □ Applying appropriate administrative and physical safeguarding/blocking all exploited ports
  - □ Notifying other Information/System Owners of the attempted breach



INCIDENT IDENTIFICATION

INCIDENT REPORTING

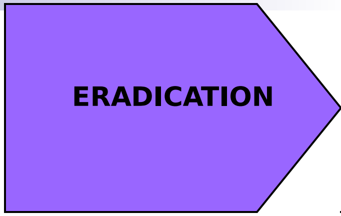
CONTAINMENT

MITIGATION

ERADICATION

RECOVERY

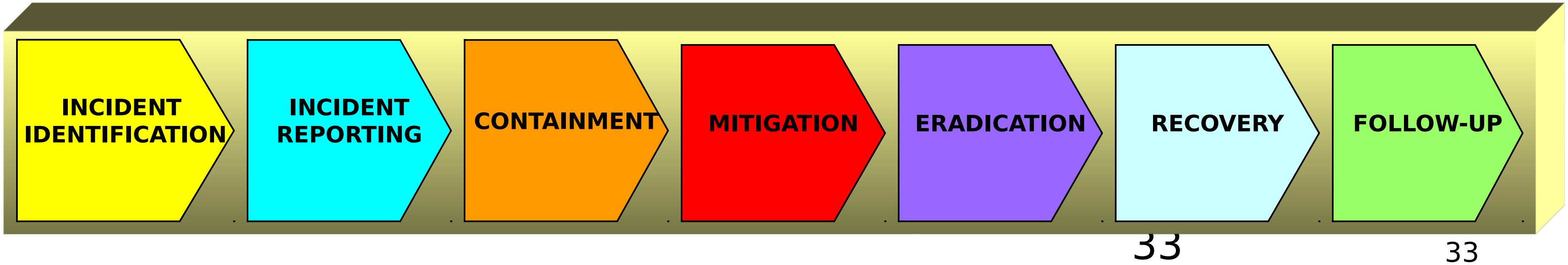
FOLLOW-UP



Breach Notification SOP Overview and Activity

# Eradication

- Eradication entails removing the cause of an incident and mitigating vulnerabilities pertaining to the incident
- Eradication activities include, at a minimum, the following:
  - **Mitigate** vulnerabilities and follow existing local and higher authority guidance regarding additional incident eradication requirements
  - **Document** eradication response actions in the incident identification log

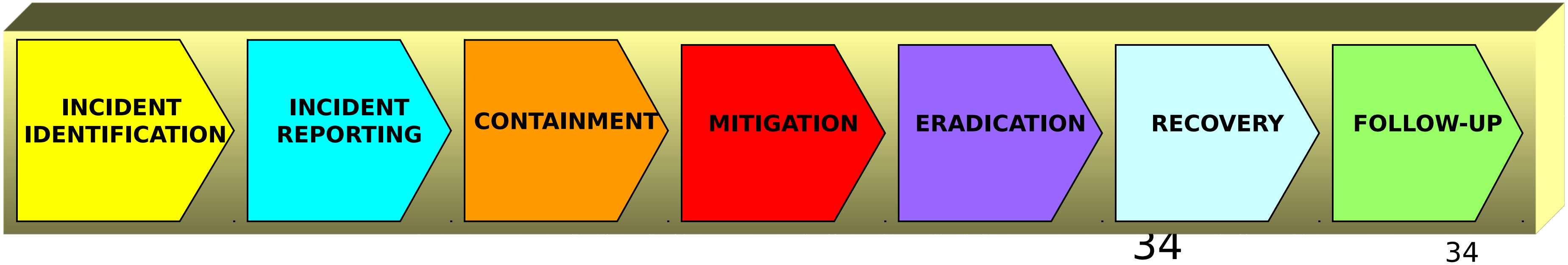


RECOVERY

Breach Notification SOP Overview and Activity

# Recovery

- Recovery is the process of restoring to normal the status that existed prior to the occurrence of the incident
  - **Verify** that any restoration actions were successful and that the operational status has been returned to its normal condition
  - **Document** recovery response actions in the incident identification log

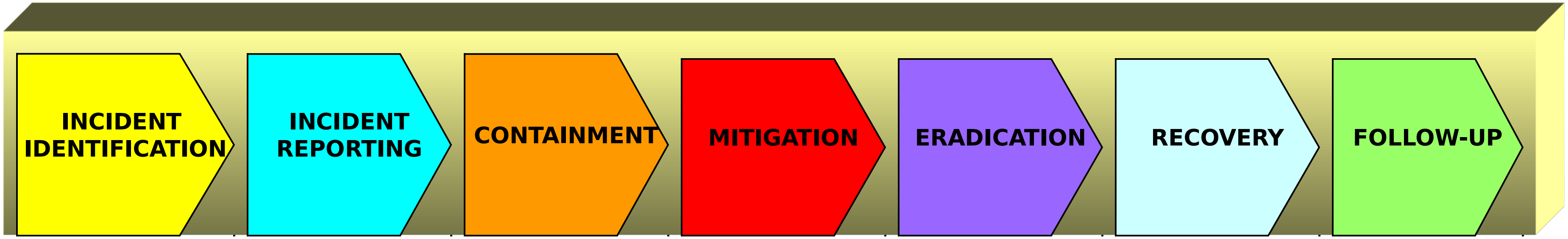


Breach Notification SOP Overview and Activity

# Follow-up

FOLLOW-UP

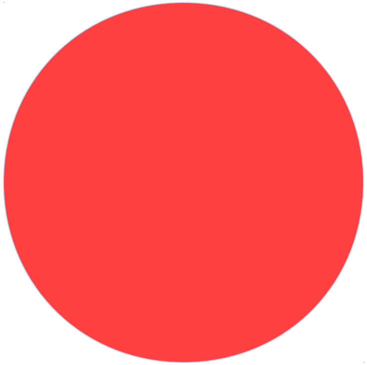
- Follow-up is a critical step in the incident response process because it assists with the response to, and prevention of, future incidents
  - □ **Develop lessons learned** with interviews and review of incident response
  - □ **Update your Incident Response Program** that can assist with the response to, and prevention of, future incidents based on the lessons learned


INCIDENT IDENTIFICATION → INCIDENT REPORTING → CONTAINMENT → MITIGATION → ERADICATION → RECOVERY → FOLLOW-UP

Breach Notification SOP Overview and Activity

# The Main Sections of the SOP

**Enclosures**



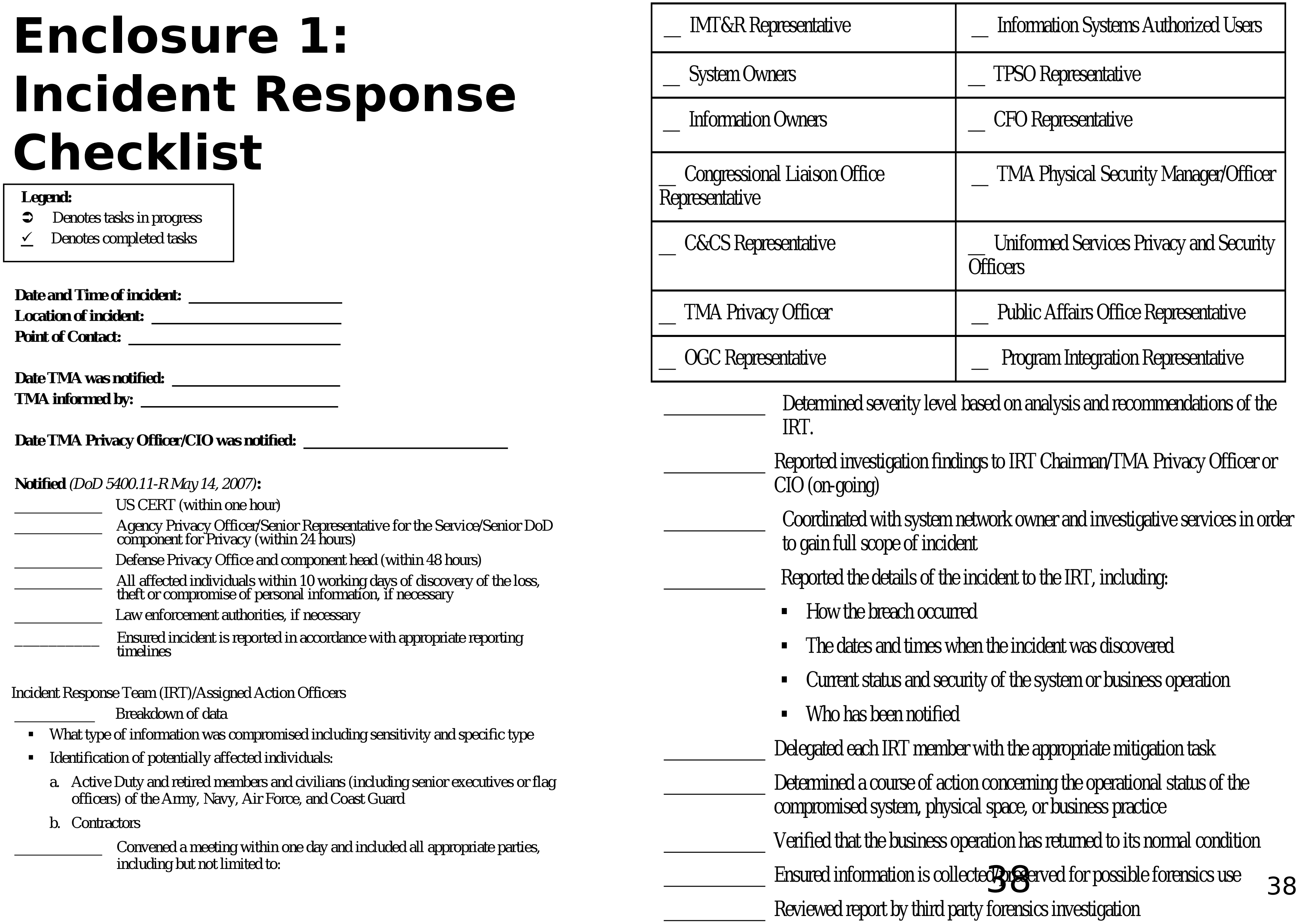
Breach Notification SOP Overview and Activity

# Enclosures

- This section provides various notification and reporting templates as guidance with completion of the requirements stated within the SOP

# Breach Notification SOP Overview and Activity

## Enclosure 1: Incident Response Checklist



**Legend:**
➲ Denotes tasks in progress
✓ Denotes completed tasks

**Date and Time of incident:** ____________________
**Location of incident:** ________________________
**Point of Contact:** ___________________________

**Date TMA was notified:** _____________________
**TMA informed by:** __________________________

**Date TMA Privacy Officer/CIO was notified:** __________________________

**Notified** *(DoD 5400.11-R May 14, 2007)***:**

___________ US CERT (within one hour)

___________ Agency Privacy Officer/Senior Representative for the Service/Senior DoD component for Privacy (within 24 hours)

___________ Defense Privacy Office and component head (within 48 hours)

___________ All affected individuals within 10 working days of discovery of the loss, theft or compromise of personal information, if necessary

___________ Law enforcement authorities, if necessary

___________ Ensured incident is reported in accordance with appropriate reporting timelines

Incident Response Team (IRT)/Assigned Action Officers

__________ Breakdown of data

- What type of information was compromised including sensitivity and specific type
- Identification of potentially affected individuals:
  a. Active Duty and retired members and civilians (including senior executives or flag officers) of the Army, Navy, Air Force, and Coast Guard
  b. Contractors

___________ Convened a meeting within one day and included all appropriate parties, including but not limited to:

| | |
|---|---|
| __ IMT&R Representative | __ Information Systems Authorized Users |
| __ System Owners | __ TPSO Representative |
| __ Information Owners | __ CFO Representative |
| __ Congressional Liaison Office Representative | __ TMA Physical Security Manager/Officer |
| __ C&CS Representative | __ Uniformed Services Privacy and Security Officers |
| __ TMA Privacy Officer | __ Public Affairs Office Representative |
| __ OGC Representative | __ Program Integration Representative |

____________ Determined severity level based on analysis and recommendations of the IRT.

____________ Reported investigation findings to IRT Chairman/TMA Privacy Officer or CIO (on-going)

____________ Coordinated with system network owner and investigative services in order to gain full scope of incident

____________ Reported the details of the incident to the IRT, including:

- How the breach occurred
- The dates and times when the incident was discovered
- Current status and security of the system or business operation
- Who has been notified

____________ Delegated each IRT member with the appropriate mitigation task

____________ Determined a course of action concerning the operational status of the compromised system, physical space, or business practice

____________ Verified that the business operation has returned to its normal condition

____________ Ensured information is collected/preserved for possible forensics use

____________ Reviewed report by third party forensics investigation

## Breach Notification SOP Overview and Activity

# Enclosure 1: Incident Response Checklist

____________ Created and provided a chronology and notebook of the incident, including:

- Summary of incident
- Meeting minutes
- Updates to senior leadership
- Executive Summaries
- Reports to external agencies, as necessary
- Establish a POA&M
- Notebook of chronology of action taken, to include executive summaries, leadership updates, e-mail communication, letters, incident reports, meeting minutes for documentation/historical purposes.

____________ Ensured that IRT members received all information in a timely manner through meetings and e-mails

____________ TMA shall determine whether TMA and/or the contractor shall make the required notification

__ Contractor obtains TMA approval of notification letters

____________ POC for DMDC to obtain the address information, e-mail address, and phone numbers of the affected individuals and ensured that these addresses are used in the mailings

____________ Ensured a call center is established to provide responses to individuals who have additional questions/concerns

____________ Ensured a Web site is developed that included:

- Frequently Asked Questions
- General notification information
- Information concerning identity theft, along with contact information for credit bureaus

____________ Drafted notification letter (C&CS)

__ Obtain approval from Incident Response Team

__ Coordination into Livelink

__ Director, TMA, determines who signs final notification letter

____________ Final notification letter signed

____________ Packaged notification letters, to include all necessary enclosures and attachments mailed out

____________ Assisted DMDC in gathering information pertaining to those individuals for whom notification letters were returned

____________ Assisted in the development of exception reports for those individuals without address information

____________ Ensured press releases are prepared and issued (Responsible Party – PAO)

____________ Provided guidance regarding Chain of Custody and certification of data destruction policies for IRT Manager

____________ Assisted the CFO in estimating the costs of the incident to include notifying the affected individuals

- Assessed financial implications of the incident
- Developed cost data associated with damage and risk mitigation
- Allocated required resources in terms of funding to respond to the incident
- Assigned financial responsibility

____________ Ensured all involved parties completed their tasks as outlined in the designated time frames

____________ Ensured lessons learned are documented

____________ Coordinated debrief/lessons learned for senior leadership

____________ Developed a comprehensive final report (After Action Report)

# Enclosure 11: Sample Notification Letter

Today’s Date

Dear Mr. John Miller:

On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand.   The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program.  The compromised information is the name, Social Security Number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain.  Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur.  We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/idtheft/con_steps.htm. The FTC urges that you immediately place an initial fraud alert on your credit file.  The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call ____________________.

# Activity

# Breach Prevention

# Best Practices for Pre-Breach Activities

- Review and update contracts to ensure that Business Associate Agreement language is included and up-to-date
- Perform frequent workforce training on breach notification
- Develop internal breach notification policies and procedures
- Create a breach response team and assign roles and responsibilities to the team members
- Maintain a current listing of key Points of Contact
- Perform annual drills of breach response activities

Breach Notification SOP Overview and Activity

# Best Practices for Pre-Breach Activities (continued)

- Be aware of all guidance documents related to breach reporting and notification
- Ensure that internal procedures are revised accordingly upon receipt of any new guidance documents
- Always review Lessons Learned from previous breach response activities with your staff to ensure proper handling of future occurrences
- Remember that breach guidance and reporting forms are readily available on the TMA Privacy Office Website:
  - http://www.tricare.mil/tmaprivacy/downloads/Breach-Guidance.doc
  - http://www.tricare.mil/tmaprivacy/downloads/Breach-Rpt.doc

Breach Notification SOP Overview and Activity

# Summary

- You now can:
  - Explain the key elements of breach response and notification
  - Define your role in identifying and responding to breaches
  - Describe how to prevent breaches and protect your identity